Analytical Optimal Solution of Selfish Node Detection with 2-hop Constraints in OppNets: A Pontryagin's Maximum Principle Approach

Yang Gao[1], Jun Tao[1], Zuyan Wang[1], and Wenqiang Li[1]

[1]School of Cyber Sci. & Engr., Southeast University, Nanjing, China
Email: {yanggao, juntao, zuyan94, wqli}@seu.edu.cn

***Abstract*—Selfish node detection offers an effective means to mitigate the routing performance degradation caused by selfish behaviors in Opportunistic Networks (OppNets), but leads to the extra network overload and computation cost. Most existing effort in the literature focuses on exploring the detection methods based on the traffic analysis or the cooperations among nodes. In this paper, we investigate the state transition of nodes in the message dissemination without detection. Specifically, the Ordinary Differential Equation (ODE) is constructed to approximatively model the periodic detection with complete detection requirement. Then we propose the optimal detection solution with the Pontryagin's maximum principle, and mathematically deduce the right detection time during the message lifetime. The model soundness is verified statistically and the analysis accuracy is evaluated via extensive simulations. The experiments also show that our solution can achieve the tradeoff between the reward and the detection cost.**

***Index Terms*—Selfish Node Detection, Ordinary Differential Equation, Pontryagin's Maximum Principle**

I. Introduction

Opportunistic networks (OppNets) have been attracting the research attentions in the recent years, which are usually exploited to provide the communication service as the valid complement of the cellular network, especially in the remote areas and in the emergency situations [1]–[4]. With the popularity of mobile communication devices, various OppNet-based applications [1], [2] are designed and deployed in the academia and industry besides the traditional advertisement and communication application. [1] presented a venue recommendation platform OmniSuggest based on OppNets, which exploited the mobility pattern to achieve the optimal recommendations. Inspired by the message forwarding in OppNets, the computation offloading framework, which integrates the incentive scheme and the reputation mechanism, was proposed to reduce the execution time and energy consumption in the scenarios without cellular infrastructures [2].

Much research effort on the routing schemes exist in the literature, where the message dissemination performance dominates the applications of OppNets [5]–[8]. However, the selfish behavior is also the bottleneck of the routing performance besides the routing methods, especially considering that the message carrying service will occupy the limited energy and memory of the. Thus how to suppress the selfish behaviors becomes another critical issue in OppNets.

A valid methodology to mitigate the selfish behaviors is conducting the selfish node detection. The state-of-the-art detection schemes can be divided into two categories in light of their aims: watchdog systems [9]–[12] and social trust-based communications [13]–[15]. The former intends to detect selfish behavior by analyzing the traffic received from their contacted nodes, while the latter establishes social trust relationships to select trusted and secured relay nodes. Most of these works, either watchdog system methods or social trust-based communicating approaches, are micro-perspective studies, lead to network management cost due to the detecting expense, and introduce extra detection traffic, degrading the overall performance of OppNets.

Incentive methods, i.e., reward, are often exploited to attract the cooperations of nodes. But the selfish nodes can pretend to carry the message and gain the reward by cheating at the same time. The detection can decrease the impact of selfish behaviors effectively. However, the detection also introduces the detection cost, including the computation cost and the communication cost. In this paper, we exploit the Pontryagin's maximum principle to minimize the weighted cost of the detection and the reward based on the constructed message dissemination model. The main contributions are as follows.

- we formulate the ordinary differential equation model (ODE) to capture and analytically evaluate the state transition of nodes in OppNets without detection and with complete detection.
- we propose an optimal solution of selfish node detection based on the Pontryagin's maximum principle to achieve the tradeoff between the detection cost and the reward of selfish behaviors.
- we conduct experiments to evaluate the effectiveness of the proposed model and the optimal selfish detection solution in terms of the total cost, the wasted reward and the node state transition.

The rest of this paper is organized as follows. The literature is reviewed in Section II. We formulate the problem in Section III. The change of network state without detection and with fully detection is investigated in Section IV. The optimal solution of the selfish detection in OppNets is presented in Section V, and evaluated in Section VI. The paper concludes

in Section VII.

II. Related Work

OppNets, which face two challenges, i.e., energy efficiency and network management cost minimization are expected to accommodate participants with low-delay and cost-effective services. Therefore, many research works targeted to address these issues.

A. Message Transmission in OppNets

In order to mitigate the performance degradation caused by the selfish behaviours in OppNets, much effort has been made to explore the methods of selfish node detection [7], [16]. An early investigation on the selfish behaviour detection is [9], where the watchdog nodes were proposed to analyze the traffic received from their encountered nodes. This work was extended for applications with the elimination of the limited knowledge on node detection by single watchdog, and the cooperative systems with multiple watchdogs were proposed in [10]–[12]. [10] proposed a collaborative approach (CoCoWa, Collaborative Contact-based Watchdog), which considered the diffusion of local selfish nodes awareness, to conduct the selfish node detection in MANETs. Through accelerating the information propagation, the method improved the performance of selfish node detection in terms of the time and the precision. [12] proposed a social-based watchdog system (SoWatch), with a watchdog module to protect SoWatch against the wrong watchdogs manipulated by malicious nodes.

Another kind of approach tries to establish social trust relationships between mobile nodes in OppNets by leveraging their online social information (explicit trust) as well as their interactions or mobility properties (implicit trust). In [13], a probabilistic misbehavior detection scheme(iTrust), which introduced a periodically available Trusted Authority(TA), was presented to judge a node's behaviour. Another trust framework PROVEST (PROVEnance-baSed Trust model) that aimed to achieve accurate peer-to-peer trust assessment was presented in [14]. The partial selfishness was investigated and credit-based algorithm to measure the degree of selfishness was designed in [15].

[17] combined watchdog technique with trust-based communications and integrated with PRoPHET to build a global perception of forwarding behavior for detection of selfish nodes. [18] introduced ensemble learning for environment-adaptive malicious node detection. [19] integrated buffer-aided full-duplex/half-duplex relaying with non-orthogonal multiple access(BAHyNOMA) for relay selection.

Routing is a critical bottleneck when selfish behaviour is exhibited and a potential alleviation is to develop incentivizing mechanisms for message forwarding. Incentive-based protocols, such as SEIR [20], Multicent [21], were devised to increase node participation in message forwarding by opting for mechanisms that reward active participation of nodes in the forwarding of messages and penalize them otherwise. To balance the tradeoff between the delivery rate and forwarding cost, game theory was introduced to optimize the configuration in MANET for more efficient energy-aware routing in [22]. While geo-casting routing protocols like LoSeRo [23] exploited the location data to enhance the message routing performance, onion-based anonymous routing approach [24] and ePRIVO [25] were proposed to keep users' information private. For MOSNs, which exhibits a nested core-periphery hierarchy(NCPH), [26] presented an up-and down routing protocol to upload message from source node to the network core and then download to the destination. [27] proposed a context-aware self-adaptive routing protocol that is able to adapt to different scenarios.

B. Optimizations of OppNets

Due to the openness of the wireless communication and the limitations of the 'store-carry-forward' paradigm, the performance of data delivery in OppNets may be reduced by abnormal behaviors. For example, the selfish behavior will highly degrade the efficiency of data offloading and the malicious behaviors will disrupt the normal communications between the nodes and the network throughput severely [7]. It is critical to identify the abnormal node behaviors from network accurately and promote these nodes to participation in collaboration and resource sharing.

Observing the importance of selfish behaviour detection schemes for the OppNets, a lot of efforts were put into its design [12], [14], [28]–[30]. In [12], a general altruism model, called SoWatch, was utilized to distinguish individually selfish behaviour and socially selfish behaviour. It also showed that the individual and social preferences of selfish nodes may mitigate the cooperation in data relaying. An incentive-driven and fresh-ness-aware pub/sub content dissemination scheme was proposed in [28], with the objective of maximizing the utility of the content inventory stored in node's buffer. [29] proposed a dynamic trust management protocol, in which 'healthiness' and 'unselfishness' are considered as two social trust metrics. A more comprehensive set of performance metrics to characterize QoS in the OppNets was investigated in [14]. To guaranty the security requirements of the OppNets, a credit-based rewarding scheme was proposed in [30].

On the other hand, the protection and defense mechanisms for malicious behaviors have been demanded by the OppNets. To deal with the blackhole and greyhole attacks in DTN, [31] proposed a statistical-based detection scheme and demonstrated its high accuracy. A compositional secured routing algorithm for the DTNs was proposed in [32], where the information list of malicious nodes was delivered by the trusted nodes. The types and effectiveness of Sybil attacks in OppNets was introduced by [33], with the consideration of various resource and attack boosting graph faking attempts. The problem of crisis of confidence caused by malicious nodes was proposed in [34], and a dynamic trust management model was presented there to solve the problem. In [35], an adaptive trust management protocol for social IoT systems was proposed to choose the trust parameter settings and change node's social conditions.

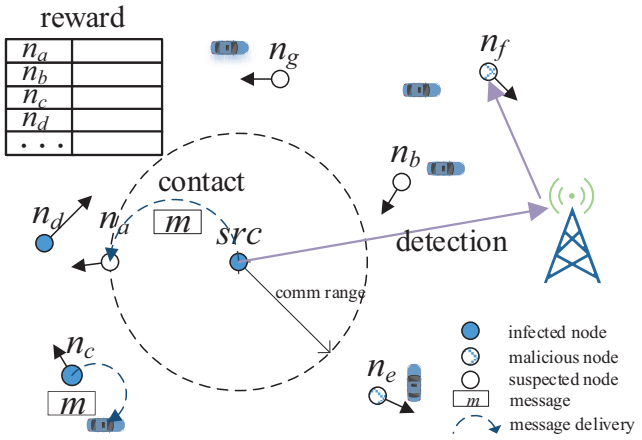

Fig. 1. Reward and Detection of the selfish nodes in OppNets.

Few these existing works focus on optimal control policy, while we introduce it for selfish node detection, where the scenario is different from [36] in this paper.

III. Preliminaries

The source node src needs to disseminate its message m to vehicles or pedestrians. The N relay nodes can replicate m and send it to the vehicles, which is shown in Fig. 1. Thus the potential coverage area of the message is broadened by the opportunistic network. To encourage the collaboration of relay nodes, src should reward the relay node n_i $(1 \leq i \leq N)$ based on the time, when the message are carried by n_i. The time ranges from the replication time (τ_i) to the time-to-live of the message (T). τ_i can be recorded by src when n_i contacts src and replicates m. However, n_i may discard m immediately after the contact to earn the reward without carrying m, which is the selfish behavior. So src can check the checksum of m's specific part, which is store in the randomly selected relay node n_i. If the check failed, n_i will be identified as the selfish node and can not receive the reward. In this paper, we propose the optimal randomly detection strategy to achieve the tradeoff between the cost of the random detections and the wasted reward of the selfish behaviors.

$E(R(t))$ denotes the expected number of the relay nodes, which have not contacted src before time t. $E(I(t))$ denotes the expected number of infected relay nodes, which still carry the message at time t. $E(D(t))$ denotes the expected number of selfish relay nodes, which have discarded the message but are not known by src at time t. Similar to [37] and [38], the contacts between each pair of nodes including src are assumed to occur according to the Poisson process, in which the contact rate is λ. The total number of relay nodes is N, and $N = R(t) + I(t) + D(t)$, $\forall t$, $0 \leq t \leq T$. We also assume the change rate of becoming the selfish node is a constant value ρ. The detection rate is $U(t)$, $0 \leq U(t) \leq U_m$, $\forall t$, $0 \leq t \leq T$. which is the control function. For example, if the minimal circle of once detection T_m is that 2 seconds, the maximal detection rate is that $U_m = \frac{1}{T_m} = 0.5$ times per second. To simplify the denotations, we use $R(t)$, $I(t)$ and $D(t)$ to replace $E(R(t))$, $E(I(t))$ and $E(D(t))$, respectively. Then the main objective of our work is to to solve the following problem,

$$Min : J = \int_0^T (1-\alpha)D(t) + \alpha U(t)dt, \tag{1}$$

which minimizes the linear combination of the wasted reward and the detection cost through the weight α, $0 \leq \alpha \leq 1$. We can also get the total paid reward is

$$P = \int_0^T \beta(I(t) + D(t))dt, \tag{2}$$

where β is the reward paid for the one node's message carrying in a unit of time.

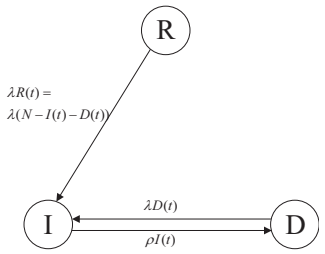

Fig. 2. State transition of the relay nodes without detection.

IV. Message Dissemination Model

We investigate the selfish detection in this and the following sections. Specifically, in this section, the ordinary differential equation model is constructed to capture the state transition and the message dissemination without detection and with complete detection.

A. Case 1: without detection

In the case without detection, the relay node with message can become the selfish node, but the selfish detection is not conducted by src. Then the state transition is shown in Fig. 2 with the following rules. The nodes change from state R to state I if they contact src. The corresponding incremental rate of state I is $\lambda R(t)$ at time t. Since the selfish node may also contact src with the contact rate λ, the rate of change from state D to state I is $\lambda D(t)$. Because $N = R(t) + I(t) + D(t)$, the total incremental rate of $I(t)$ is $\lambda(R(t) + D(t)) = \lambda(N - I(t))$. Additionally, the rate of change from state I to state D is $\rho I(t)$. We can obtain the derivative of $I(t)$ with respect to time t, $\frac{\mathrm{d}I(t)}{\mathrm{d}t} = \lambda(N - I(t)) - \rho I(t)$. Similar to $\frac{\mathrm{d}I(t)}{\mathrm{d}t}$, we can get the derivative of $D(t)$ and the derivative of $R(t)$ respectively, i.e., $\frac{\mathrm{d}D(t)}{\mathrm{d}t}$ and $\frac{\mathrm{d}R(t)}{\mathrm{d}t}$. Thus the state transition can be represented as

$$\begin{aligned} \frac{\mathrm{d}I(t)}{\mathrm{d}t} &= \lambda(N - I(t)) - \rho I(t), \\ \frac{\mathrm{d}D(t)}{\mathrm{d}t} &= -\lambda D(t) + \rho I(t), \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} &= -\lambda(N - I(t) - D(t)). \end{aligned} \tag{3}$$

Since $I(t)$ in (3) is formed by the first-order first-power ordinary differential equations (ODE) [38], we can obtain the general solutions of $I(t)$, that is,

$$I(t) = C_I e^{-(\lambda+\rho)t} + \frac{\lambda N}{\lambda + \rho}.$$

Note that $I(0) = 0$, $D(0) = 0$ and $R(0) = N$, which means only src carries the message at time 0. Thus $C_I = \frac{-\lambda N}{\lambda+\rho}$, and

$$I(t) = \frac{\lambda N}{\lambda+\rho}(1 - e^{-(\lambda+\rho)t}),$$

where $0 \leq t \leq T$. Similarly, we can calculate the general solution of the first-order ODE $D(t)$ from $\frac{\mathrm{d}D(t)}{\mathrm{d}t} + \lambda D(t) = \rho I(t)$,

$$\begin{aligned} D(t) &= C_D e^{-\int \lambda dt} + e^{-\int \lambda dt} \int \rho I(t) e^{\int \lambda dt} dt \\ &= C_D e^{-\lambda t} + \frac{\lambda N}{\lambda+\rho} e^{-(\lambda+\rho)t} + \frac{\rho N}{\lambda+\rho}. \end{aligned} \tag{4}$$

Because of $D(0) = 0$,

$$D(t) = -N e^{-\lambda t} + \frac{\lambda N}{\lambda+\rho} e^{-(\lambda+\rho)t} + \frac{\rho N}{\lambda+\rho}.$$

Since $I(t) + D(t) + R(t) = N$, $0 \leq t \leq T$, $R(t)$ can be computed based on the solved solution of $I(t)$ and $D(t)$. Thus the solution of (3) can be derived as

$$\begin{aligned} I(t) &= \frac{\lambda N}{\lambda+\rho}(1 - e^{-(\lambda+\rho)t}), \\ D(t) &= N(\frac{\lambda e^{-(\lambda+\rho)t} + \rho}{\lambda+\rho} - e^{-\lambda t}), \\ R(t) &= N e^{-\lambda t}, \end{aligned} \tag{5}$$

which depicts the change of the states when the time ranges from 0 to T. And $I(t)$, $D(t)$, $R(t) \geq 0$ always hold when $t \geq 0$. From the solutions of $I(t)$, $D(t)$ and $R(t)$, we can find that $I(t) \to \frac{\lambda N}{\lambda+\rho}$, $D(t) \to \frac{\rho N}{\lambda+\rho}$ and $R(t) \to 0$, when $t \to +\infty$. To verify the validity of the ODE model (3), we conduct the simulations with randomly settings. The corresponding results are presented in Section. VI-A.

The cost J in (1) also can be calculated based on (5). Note that $U(t) = 0$, $\forall t$, in the case without detection. J is determined by the expected number of selfish nodes $D(t)$, $0 \leq t \leq T$, which is proportional to the reward consumed by selfish behaviors. Thus J can be computed as

$$\begin{aligned} J &= \int_0^T (1-\alpha) D(t) dt, \\ &= \int_0^T (1-\alpha) N(\frac{\lambda e^{-(\lambda+\rho)t} + \rho}{\lambda+\rho} - e^{-\lambda t}) dt, \\ &= N(1-\alpha)\left(\frac{\lambda(1 - e^{-(\lambda+\rho)T})}{(\lambda+\rho)^2} + \frac{\rho T}{\lambda+\rho} - \frac{1 - e^{-\lambda T}}{\lambda}\right). \end{aligned} \tag{6}$$

Similarly, we can get the total paid reward in this case

$$P = \beta \int_0^T I(t) + D(t) dt = N\beta(T - \frac{1 - e^{-\lambda T}}{\lambda}).$$

Furthermore, the fraction between the wasted reward and the total paid reward can be obtained as

$$p = \frac{\int_0^T D(t) dt}{\int_0^T I(t) + D(t) dt} = \frac{\frac{\lambda(1-e^{-(\lambda+\rho)T})}{(\lambda+\rho)^2} + \frac{\rho T}{\lambda+\rho} - \frac{1-e^{-\lambda T}}{\lambda}}{T - \frac{1-e^{-\lambda T}}{\lambda}}.$$

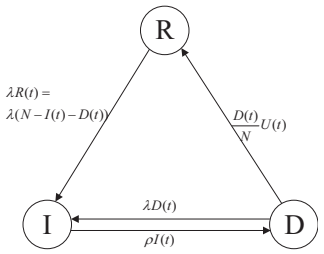

Fig. 3. State transition of the relay nodes.

B. Case 2: with complete detection

In the case with complete detection, src conducts the selfish node detection in the whole message lifetime. The detections are conducted at time T_m, $2T_m$, $\cdots$, kT_m, where $kT_m \leq T < (k+1)T_m$. In every detection, a randomly selected node n_i is checked by src whether n_i is a selfish node. We can find that the decrement of selfish node number only occurs at the instant iT_m in the case with complete detection.

In order to simplify the model, we exploit a continuous manner to describe this case with complete detection. Considering that the checked relay node is randomly selected from the N node set, we calculate the probability of selecting a selfish node as $\frac{D(t)}{N}$. Since the detection rate is constrained by $U(t)$, we let $\frac{D(t)}{N} U(t)$ denote the change rate from state D to state R caused by detections. Thus the state transition of the fully detection case is constructed as Fig. 3. The approximate model of the state transition in the case with complete detection will be constructed as

$$\begin{aligned} \frac{\mathrm{d}I(t)}{\mathrm{d}t} &= \lambda(N - I(t)) - \rho I(t), \\ \frac{\mathrm{d}D(t)}{\mathrm{d}t} &= -\lambda D(t) + \rho I(t) - \frac{D(t)}{N} U(t), \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} &= -\lambda(N - I(t) - D(t)) + \frac{D(t)}{N} U(t), \end{aligned} \tag{7}$$

based on the model in the case without detection (3). Here $U(t) = U_m$, $\forall t$, $0 \leq t \leq T$. The initial state is that $I(0) = D(0) = 0$ and $R(0) = N$. So the solution of $I(t)$, which does not change from (5), is that $I(t) = \frac{\lambda N}{\lambda+\rho}(1 - e^{-(\lambda+\rho)t})$. From $\frac{\mathrm{d}D(t)}{\mathrm{d}t} + (\lambda + \frac{U_m}{N}) D(t) = \rho I(t)$, we can derive that

$$\begin{aligned} &D(t) \\ =&C_{2D} e^{\int -(\lambda + \frac{U_m}{N}) dt} + e^{\int -(\lambda + \frac{U_m}{N}) dt} \int \rho I(t) e^{\int (\lambda + \frac{U_m}{N}) dt} dt \\ =&C_{2D} e^{-(\lambda + \frac{U_m}{N})t} - \frac{\rho\lambda N}{(\lambda+\rho)(\frac{U_m}{N} - \rho)} e^{-(\lambda+\rho)t} + \frac{\rho\lambda N}{(\lambda+\rho)(\lambda + \frac{U_m}{N})}. \end{aligned}$$

Since $D(0) = 0$ and $I(t) + D(t) + R(t) = N$, the solution

of (7) can be calculated as

$$\begin{aligned} I(t) =& \frac{\lambda N}{\lambda+\rho}(1-e^{-(\lambda+\rho)t}), \\ D(t) =& \frac{\rho\lambda N}{(\lambda+\rho)(\lambda+\frac{U_m}{N})} + \frac{\rho\lambda N}{(\lambda+\frac{U_m}{N})(\frac{U_m}{N}-\rho)}e^{-(\lambda+\frac{U_m}{N})t} \\ & - \frac{\rho\lambda N}{(\lambda+\rho)(\frac{U_m}{N}-\rho)}e^{-(\lambda+\rho)t}, \\ R(t) =& N - \frac{\lambda N}{\lambda+\rho}\left(\frac{\rho}{\lambda+\frac{U_m}{N}}+1\right) + \frac{\lambda U_m}{(\lambda+\rho)(\frac{U_m}{N}-\rho)}e^{-(\lambda+\rho)t} \\ & - \frac{\rho\lambda N}{(\lambda+\frac{U_m}{N})(\frac{U_m}{N}-\rho)}e^{-(\lambda+\frac{U_m}{N})t}. \end{aligned} \tag{8}$$

We can find that $I(t) \to \frac{\lambda N}{\lambda+\rho}$, $D(t) \to \frac{\rho\lambda N}{(\lambda+\rho)(\lambda+\frac{U_m}{N})}$, and $R(t) \to N - \frac{\lambda N}{\lambda+\rho}\left(\frac{\rho}{\lambda+\frac{U_m}{N}}+1\right)$ when $t \to +\infty$ according to (8). Here $R(+\infty) \neq 0$ in the steady state is caused by the complete selfish detection. Based on the approximate model (7) and the corresponding solutions (8), the estimation of the total cost $\hat{J}$ can be computed as

$$\begin{aligned} \hat{J} =& \int_0^T (1-\alpha)D(t) + \alpha U(t)dt, \\ =& \frac{(1-\alpha)\rho\lambda NT}{(\lambda+\rho)(\lambda+\frac{U_m}{N})} - \frac{(1-\alpha)\rho\lambda N}{(\lambda+\frac{U_m}{N})^2(\frac{U_m}{N}-\rho)}(e^{-(\lambda+\frac{U_m}{N})T}-1) \\ & + \frac{(1-\alpha)\rho\lambda N}{(\lambda+\rho)^2(\frac{U_m}{N}-\rho)}(e^{-(\lambda+\rho)T}-1) + \alpha T U_m. \end{aligned} \tag{9}$$

The reason why (9) is the estimation of the cost is that the decrement of $D(t)$ actually occurs in the end of the detection cycle. However, the change rate of $D(t)$ in (7) is denoted by $\frac{D(t)}{N}U(t)$ in the above analysis. So there exists a deviation between the true cost J and the estimated cost $\hat{J}$ in the case with complete detection.

Lemma 1. *When $t \to +\infty$, $T_m \ll T$, a deviation between $D(t)$ in the approximate model (8) and in the real scenario is limited.*

Proof. At first we discuss the real scenario of the complete detection case. Without loss of generality, assume that $(0, T)$ can be divided into k detection cycles and a following duration t_{k+1}. Here the i-th detection cycle is denoted by $(t_{i-1}, t_i]$, where $t_i - t_{i-1} = T_m$ and $t_{k+1} < T_m$. In every detection cycle, $D(t)$ increases from $D(t_{i-1})$ to $D(t_i^-)$ in (t_0, t_1^-). Since the detection occurs at the instant t_i, $D(t_i^+) = \frac{N-1}{N}D(t_i^-)$. From (5) we can find that $D(t)$ increases with time in the case and approaches to the stable state in the case without detection. In the case with complete detection, when $t \to +\infty$, $D(t)$ also approaches to the stable state, where $D(t_{i-1}^+) = D(t_i^+)$. We can obtain that

$$\begin{aligned} D(t_{i-1}^+) =& C_i e^{-\lambda t_{i-1}^+} + \frac{\lambda N}{\lambda+\rho}e^{-(\lambda+\rho)t_{i-1}^+} + \frac{\rho N}{\lambda+\rho}, \\ D(t_i^-) =& C_i e^{-\lambda t_i^+} + \frac{\lambda N}{\lambda+\rho}e^{-(\lambda+\rho)t_i^+} + \frac{\rho N}{\lambda+\rho}, \end{aligned}$$

in (t_{i-1}, t_i) based on (4). Then, when $i \to +\infty$,

$$\begin{aligned} D(t_i^+) =& \frac{N-1}{N}D(t_i^-) \\ =& \frac{N-1}{N}D(t_{i-1}^+)e^{-\lambda T_m} + \frac{\rho(N-1)}{\lambda+\rho}(1-e^{-\lambda T_m}) \end{aligned}$$

Considering that $D(t_{i-1}^+) = D(t_i^+)$, we can get that

$$\begin{aligned} \lim_{i\to+\infty} D(t_i^+) &= \frac{\rho(N-1)}{\lambda+\rho}\frac{1-e^{-\lambda T_m}}{(1-\frac{N-1}{N}e^{-\lambda T_m})} \\ \lim_{i\to+\infty} D(t_i^-) &= \frac{\rho N}{\lambda+\rho}\frac{1-e^{-\lambda T_m}}{(1-\frac{N-1}{N}e^{-\lambda T_m})} \end{aligned}$$

According to (8), $D(+\infty) = \frac{\rho\lambda N}{(\lambda+\rho)(\lambda+\frac{U_m}{N})}$. Since these limitations are the limited values related to ρ, λ, N and U_m, the deviation of $D(t)$ between in the approximate model and in the real scenario is limited. □

Lemma 2. *Let J denote the cost in the complete detection case. In the case with fully detection, $|J - \hat{J}|$ is less than $(1-\alpha)TN$.*

Proof. Considering that $U(t) = \hat{U}(t) = U_m$, we can derive that $\int_0^T U(t)dt = TU_m = \int_0^T \hat{U}(t)dt$. And the deviation between the estimated cost and the true cost

$$\begin{aligned} |J - \hat{J}| =& \left| \int_0^T (1-\alpha)D(t)dt - \int_0^T (1-\alpha)\hat{D(t)}dt \right| \\ \leq& (1-\alpha)\int_0^T |(D(t) - \hat{D(t)})|dt \\ \leq& (1-\alpha)TN \end{aligned} \tag{10}$$

where $0 \leq D(t), \hat{D(t)} \leq N$.

□

We also can compute the approximate total reward is

$$\begin{aligned} \hat{P} =& \beta\int_0^T I(t) + D(t)dt, \\ =& \frac{\beta\rho\lambda NT}{(\lambda+\rho)(\lambda+\frac{U_m}{N})} - \frac{\beta\rho\lambda N}{(\lambda+\frac{U_m}{N})^2(\frac{U_m}{N}-\rho)}(e^{-(\lambda+\frac{U_m}{N})T}-1) \\ & + \frac{\beta\rho\lambda N}{(\lambda+\rho)^2(\frac{U_m}{N}-\rho)}(e^{-(\lambda+\rho)T}-1) + \frac{\lambda N}{(\lambda+\rho)^2}(e^{-(\lambda+\rho)T}-1) \\ & + \frac{\beta\lambda NT}{\lambda+\rho} \end{aligned}$$

Similarly, the utilization ratio of reward also can be obtained $\hat{p} = \frac{\int_0^T D(t)dt}{\int_0^T I(t)+D(t)dt}$. From (8) to (5), we find $I(t)$ does not change but $D(t)$ decreases. Thus this complete detection case can reduce the selfish behaviors with the additional cost of the selfish node detections, e.g., energy, bandwidth and wireless communication fee. Thus we try to achieve the tradeoff between the paid reward and the detection cost via the optimal solution.

V. Optimal Detection

A. Problem Formulation

Assume that the detection can be conducted. The detection rate is $U(t)$, $0 \leq U(t) \leq U_m$. U_m is the limitation of the detection rate, which is the constraint from the hardware and the time sequences. Then, the ODEs can be reformulated as

$$\begin{aligned} \frac{\mathrm{d}I(t)}{\mathrm{d}t} &= \lambda(N - I(t)) - \rho I(t), \\ \frac{\mathrm{d}D(t)}{\mathrm{d}t} &= \rho I(t) - \lambda D(t) - \frac{D(t)}{N}U(t), \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} &= -\beta(N - I(t) - D(t)) + \frac{D(t)}{N}U(t). \end{aligned} \tag{11}$$

Meanwhile,

$$\begin{aligned} I(0) &= 0, \\ D(0) &= 0, \\ R(0) &= N. \end{aligned} \tag{12}$$

Thus $I(t)$ is the same with that in the situation without detection, which is

$$I(t) = \frac{\lambda N}{\lambda + \rho}(1 - e^{-(\lambda+\rho)t}). \tag{13}$$

Considering that the detection is also the cost, the object function will be

$$J = \int_0^T (1-\alpha)D + \alpha U dt.$$

Here α is the weight, which can control the importance between the cost of selfish relay nodes and detections. Thus $0 < \alpha < 1$. Similar with the previous section, $I(t)$ and $D(t)$ is the state functions. $U(t)$ is the controllable variable, $0 \leq U(t) \leq U_m$.

B. Optimal Control by Pontryagin's Maximum Principle

Now we utilize the Pontryagin's maximal principle [36] to find the optimal $U(t)$, which will minimize the total cost. First, the Hamilton function is

$$\begin{aligned} H =& (1-\alpha)D + \alpha U + \lambda_I(\lambda(N-I) - \rho I) \\ &+ \lambda_D(\rho I - \lambda D - \frac{D}{N}U) \\ =& (1-\alpha)D + \lambda_I(\lambda(N-I) - \rho I) \\ &+ \lambda_D(\rho I - \lambda D) + (\alpha - \lambda_D \frac{D}{N})U. \end{aligned}$$

Note that λ_I and λ_D denote two co-state functions. Without the final constraint, the terminal condition is $\lambda_I(T) = 0$ and $\lambda_D(T) = 0$. Then the adjoint function is

$$\dot{\lambda_D} = -\frac{\partial H}{\partial D} = \lambda_D(\lambda + \frac{U}{N}) - (1-\alpha).$$

Thus

$$U^*(t) = \begin{cases} 0, & \text{if } \alpha - \lambda_D \frac{D}{N} \geq 0 \\ U_m, & \text{if } \alpha - \lambda_D \frac{D}{N} < 0 \end{cases} \tag{14}$$

In summary, we have the ODE functions $\dot{D}$, $\dot{\lambda_D}$, the initial condition $D(0) = 0$ and the boundary condition $\lambda_D(T) = 0$, Thus the problem is to solve a BVP problem, which is

$$\begin{aligned} \dot{D} &= -(\lambda + \frac{U^*}{N})D + \rho I, \\ \dot{\lambda_D} &= (\lambda + \frac{U^*}{N})\lambda_D - (1-\alpha), \end{aligned} \tag{15}$$

where $D(0) = 0$ and $\lambda_D(T) = 0$. We can solve the BVP problem with the shooting method by the bvpSolve package of R. The whole algorithm are shown in Alg. 1, where δt presents the time granularity. The message replication time τ_0 and the state switching time are recorded by src. So the reward can also be computed by src. Then we analyze the properties of the optimal control variable.

Algorithm 1 Optimal Selfish Node Detection

Require: T_m, U_m, λ, ρ, T
time $t \leftarrow 0$
compute the solution of (15) as the switch-on duration $\mathcal{T}$
while $t \leq T$ **do**
  if contact n_i without message **then**
    replicate m to n_i
    state of n_i changes to I
    record t as τ_0
  end if
  if $t \in \mathcal{T}$ **then**
    select a relay node n_j randomly
    conduct the detection of n_j
    if n_j is detected as a selfish node **then**
      state of n_j changes to R
      record t as the state switch time
    end if
  end if
  $t \leftarrow t + \delta t$
end while
for n_i, $1 \leq i \leq N$ **do**
  pay the reward to n_i based on the time of staying state I
end for

Lemma 3. *At the beginning and the end of the whole duration, the optimal control stop the selfish detection, which is* $U(0) = U(T) = 0$.

Proof. At the beginning of the duration, $M(0) = 0$, which is the initial condition of 15. Then $\alpha - \lambda_D(0)\frac{D(0)}{N} = \alpha > 0$. Following (14), the optimal $U(0) = 0$.

At the end of the duration, $\lambda_2(T) = 0$, which is the boundary condition of 15. Then $\alpha - \lambda_D(T)\frac{D(T)}{N} = \alpha > 0$. Based on (14), the optimal $U(T) = 0$. □

Based on the differential function $\dot{I}$, the equilibrium point of I can be obtained from $\dot{I} = 0$, which is $I^* = \frac{\beta N}{\beta+\rho}$. When $I(t) < I^*$, $I(t)$ will increase with t and approach to $\frac{\beta N}{\beta+\rho}$. Meanwhile, in this paper $I(0) = 0$ at the beginning of time.

Based on the differential function $\dot{D}$, the equilibrium point is obtained from $\dot{D} = 0$, which is $M^* = \frac{\rho I}{\beta + \frac{1}{N}U}$. In the situation without detection, the equilibrium point is $D^* = \frac{\rho I^*}{\beta} = \frac{\rho N}{\beta+\rho}$. In the situation with full detection, the equilibrium point is $D^* = \frac{\rho I^*}{\beta + \frac{1}{N}U_m} = \frac{\rho}{\beta + \frac{1}{N}U_m}\frac{\beta N}{\beta+\rho}$.

Since α is the weight of detecting the selfish nodes, we can assume that if α is enough high, the detection will not perform according to the optimal control strategy.

Lemma 4. *If* $\alpha \geq \alpha_{th}$, *the optimal control let the detection stop in the whole duration, namely* $U(t) = 0$, $0 \leq t \leq T$.

Proof. Assume that ρ, N, β is given. Let $W(t) = \lambda_D(t)D(t)$.

$$\begin{aligned} W^{'}(t) =& D^{'}(t)\lambda_D(t) + D(t)\lambda_D^{'}(t) \\ =& \left(\rho I(t) - \beta D(t) - \frac{D(t)}{N}U(t)\right)\lambda_D(t) \\ &+ D(t)\left(\lambda_D(t)\left(\beta + \frac{U(t)}{N}\right) - (1-\alpha)\right) \\ =& \rho\lambda_D(t)I(t) - (1-\alpha)D(t). \end{aligned} \tag{16}$$

Since $D(0) = 0$ and $\lambda_D(T) = 0$, $W(0) = W(T) = 0 < \alpha N$.

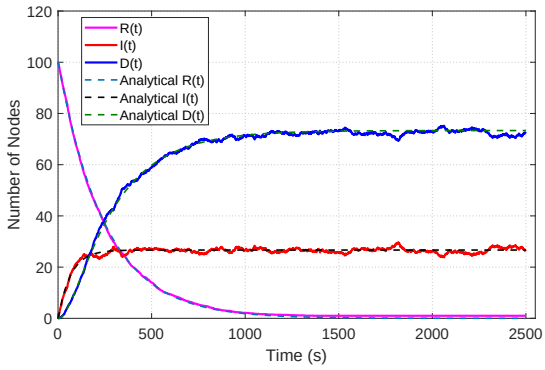

Fig. 4. Comparison of the theoretical and simulation results of the proposed ODE model in case 1.

Now we focus on the poles of $W(t)$, namely t^*, where $W^{'}(t^*) = \rho\lambda_D(t^*)I(t^*) - (1-\alpha)D(t^*) = 0$. Then $D(t^*) = \frac{\rho\lambda_D(t^*)I(t^*)}{1-\alpha}$.

$$W(t^*) = \lambda_D(t^*)D(t^*) = \frac{\rho I(t^*)\lambda_D(t^*)^2}{1-\alpha}. \tag{17}$$

According to $\dot{\lambda_D}$ in (15), the equilibrium point of λ_D is that $\lambda_D^* = \frac{1-\alpha}{\beta+\frac{U}{N}}$. Since $0 \le U \le U_m$, $0 < \frac{1-\alpha}{\beta+\frac{U_m}{N}} \le \lambda_D^* \le \frac{1-\alpha}{\beta}$. Note $\lambda_D(T) = 0$. Based on the phase line in ODE for $\dot{\lambda_D}$, $\lambda_D(t)$ decreases with t when $\lambda_D(t) < \lambda_D^*$. Conversely, $\lambda_D(t)$ increases with t when $\lambda_D(t) > \lambda_D^*$. Thus $0 \le \lambda_D(t) \le \lambda_D^* \le \frac{1-\alpha}{\beta}$ when $0 \le t \le T$. Additionally, $0 \le I(t) \le \frac{\beta N}{\beta+\rho}$. From (17), we can derive that the upper boundary of $W(t)$, W_{up}, which is

$$W(t) \le W(t^*) \le \frac{\rho}{1-\alpha}\frac{\beta N}{\beta+\rho}(\frac{1-\alpha}{\beta})^2 = \frac{\rho N(1-\alpha)}{\beta(\beta+\rho)} = W_{up}.$$

Assume that α can satisfy that $W_{up} \le \alpha N$, which means that $\alpha \ge \frac{\rho}{\beta(\beta+\rho)+\rho} = \alpha_{th}$. Then $W(t) \le \alpha N$, when $0 \le t \le T$. Therefore the optimal control $U^*(t) \equiv 0$, when $0 \le t \le T$ in this situation. □

VI. Performance Evaluation

The total number of relay nodes is 100, excluding src, which means that $N = 100$. The Poisson-contact mobility model is synthetic, where the parameter λ is set to 4×10^{-3} s^{-1}. The source node is fixed at the center of the network scenario. We set the parameter ρ as 1.1×10^{-2} s^{-1}. The weight α is limited, i.e., $\alpha \in (0, 1)$. The minimum detection cycle is that $T_m = 1$ s. Note that all statistical results in the experiments are obtained by repeating 20 times.

A. Accuracy of Modeling

As shown in Section IV, we mathematically model the state transition of nodes by the ODEs, based on which we achieve the optimal control through the Pontryagin's Maximum Principle. Thus it is critical to verify whether the proposed model can depict the state transition in the message lifetime, i.e., the expected number of nodes in state R, I and D.

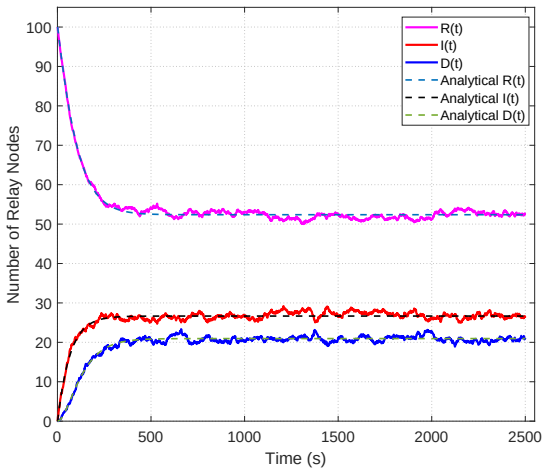

Fig. 5. Comparison of the theoretical an simulation results or the proposed ODE model in case 2.

Fig. 4 shows the comparison between the simulation and the analytical result in Case 1, where the detection are not conducted at all. Here the expected number of nodes in different states, i.e., $D(t)$, $I(t)$ and $R(t)$ are counted as the mean value of 20 simulations at t, which is the simulation result. The dotted lines represent the analytical results, which is calculated from (5) for any specific time. We can find that the analytical $I(t)$ and $D(t)$ can match the simulated $R(t)$ and $I(t)$ closely, which validates the accuracy of modeling message dissemination without detection. We notice that $I(t)$ and $D(t)$ approaches to $\frac{\lambda N}{\lambda+\rho} \approx 26.7$ and $\frac{\rho N}{\lambda+\rho} \approx 73.3$ after $1,000$ s respectively, which is conforms to the theoretical analysis.

The experiment of case 2, i.e., with complete detection is shown in Fig. 5. We can also find that $R(t)$, $I(t)$ and $D(t)$ of the mathematical analysis in (8) match that of the simulations closely, which reveals that our proposed approximately model can represents the decrement of nodes in state D caused by detections. Since the change of $I(t)$ relies on the derivative of $I(t)$, $\frac{\mathrm{d}I(t)}{\mathrm{d}t} = \lambda(N - I(t)) - \rho I(t)$, $I(t)$ is not effected by the detections according to the analysis. Thus we also find that $I(t)$ in Fig. 5 is almost equal to $I(t)$ in Fig. 4. But $D(t)$ in Fig. 5 decreases much compared to $D(t)$ in Fig. 4 due to the successive selfish node detections. Similarly, $I(t)$ and $D(t)$ approaches to $\frac{\lambda N}{\lambda+\rho} \approx 26.7$ and $\frac{\rho\lambda N}{(\lambda+\rho)(\lambda+\frac{U_m}{N})} \approx 20.9$ when $t \to +\infty$ in the steady state. Meanwhile, the analytical $I(t)$ and $D(t)$ also tend to be stable as discussed in Lemma. 1.

B. Optimal Selfish Node Detection

The weight α and the message lifetime T are set as 0.9 and 500 s, respectively. Then the corresponding numerical solution of the boundary value problem (15), i.e., $D(t)$ and $\lambda_D(t)$, is solved and shown in Fig. 6, which is the state function in the optimal solution to minimize the cost J. Here $\lambda_D(t)$ is the co-state function, which is introduced to obtain this optimal solution. Since the close-form solution of $I(t)$ is not effected

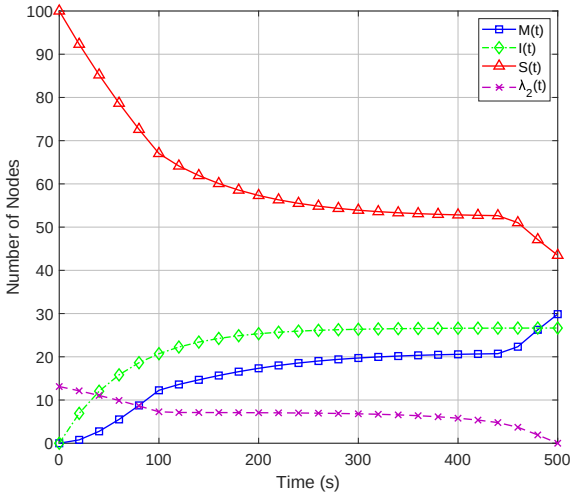

Fig. 6. State variable of analysis with time.

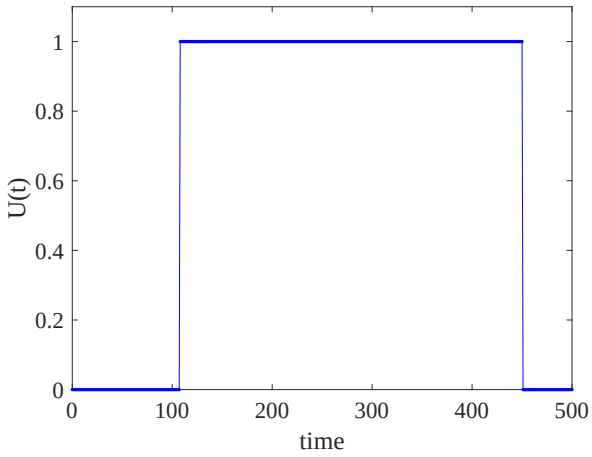

Fig. 7. The optimal control policy of $U(t)$.

by the detections, which is similar to Section. VI-A, we can get $R(t)$ according to $N = R(t) + I(t) + D(t)$.

Since $D(t)$ and $\lambda_D(t)$ in the optimal solution have been calculated, $U^*(t)$ can be obtained based on (14). Fig. 7 shows the optimal policy of the selfish node detections, when $\alpha = 0.9$ and $T = 500\ s$. As discussed in Lemma. 3, the detection is off at the start and the end of the message lifetime. [***ts tt***]. We can find that the optimal control is 'off-on-off' function. In the 'on' state of $U^*(t)$, src will conduct the self node detection with the minimum cycle T_m. But no detection will be conducted in the 'off' state of $U^*(t)$. Thus the switching time t_s and t_t, around $102\ s$ and $452\ s$, dominate the cost J in the whole simulation. Combining with Fig. 6, we can also find that $D(t)$ and $\lambda_D(t)$ is not smooth at the switching time.

[*** new line ***]. When α = is higher than α_{th} the optimal control policy $U^*(t) = 0$, $\forall t$, which is correspond to Lemma. 4.

C. Cost J v.s. Switching Time

Fig. 8 shows the total cost J with different switching time t_s and t_t, when $\alpha = 0.9$ and $T = 500\ s$. Here the combination (t_s, t_t) is greedily set from $(0, 0)$ to $(500, 500)$ Here $(t_s, t_t) = (0, 500)$ indicates the case with the complete detection. And $t_s = t_t$ represents the case without detection. in the stepwise of $10\ s$. For each specific combination (t_s, t_t), the cost J is approximately calculate with $J \approx \sum_t (1-\alpha)D(t) + \alpha U(t)$ and the time granularity of $0.1\ s$ during 20 times simulations. We can find that J ranges around from $1,400$ to $1,600$. The optimal solution of our method is that $t_s = 102\ s$ and $t_t = 402\ s$, which is labeled as '*'. Thus the proposed method in this paper can provide the near optimal solution of the selfish node detection, i.e., around the minimum cost J_{min}, in the opportunistic network.

[*** P ***] another benchmark? maybe?

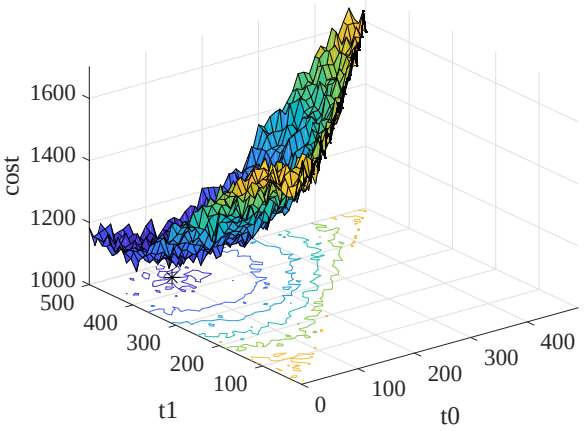

Fig. 8. Different choices of $t0$ and $t1$.

VII. Conclusion

In this paper, we have analytically investigated the state transition of nodes in the opportunistic networks. The ordinary differential equation models have been constructed to capture the message dissemination with complete detection, which can suppress the increment of selfish node number. To achieve the tradeoff the reward and the detection cost in the message lifetime, we propose the optimal solution of the selfish node detection based on the Pontryagin's maximum principle. The soundness of the models and the accuracy of the analysis have been verified via extensive simulation.

References

[1] O. Khalid, M. U. S. Khan, S. U. Khan, and A. Y. Zomaya, "Omnisuggest: A ubiquitous cloud-based context-aware recommendation system for mobile social networks," *IEEE Trans. Serv. Comput.*, vol. 7, no. 3, pp. 401–414, 2014.

[2] D. Chatzopoulos, M. Ahmadi, S. Kosta, and P. Hui, "Flopcoin: A cryptocurrency for computation offloading," *IEEE Trans. Mob. Comput.*, vol. 17, no. 5, pp. 1062–1075, 2018.

[3] B. Han, P. Hui, V. S. A. Kumar, M. V. Marathe, J. Shao, and A. Srinivasan, "Mobile data offloading through opportunistic communications and social participation," *IEEE Trans. Mob. Comput.*, vol. 11, no. 5, pp. 821–834, 2012.

[4] Y. Li, M. Qian, D. Jin, P. Hui, Z. Wang, and S. Chen, "Multiple mobile data offloading through disruption tolerant networks," *IEEE Trans. Mob. Comput.*, vol. 13, no. 7, pp. 1579–1596, 2014.

[5] C. B. Souza, E. Mota, D. Soares, P. Manzoni, J. Cano, and C. T. Calafate, "Improving delivery delay in social-based message forwarding in delay tolerant networks," in *Proceedings of the 2016 workshop on Fostering Latin-American Research in Data Communication Networks, LANCOMM@SIGCOMM 2016, Florianopolis, Brazil, August 22-26, 2016*. ACM, 2016, pp. 52–54.

[6] M. Radenkovic and V. S. H. Huynh, "Collaborative cognitive content dissemination and query in heterogeneous mobile opportunistic networks," in *Proceedings of the 3rd Workshop on Experiences with the Design and Implementation of Smart Objects, SmartObjects@MobiCom 2017, Snowbird, UT, USA, October 16, 2017*. ACM, 2017, pp. 7–12.

[7] B. Jedari, F. Xia, and Z. Ning, "A survey on human-centric communications in non-cooperative wireless relay networks," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 2, pp. 914–944, 2018.

[8] P. Loreti and L. Bracciale, "Optimized neighbor discovery for opportunistic networks of energy constrained iot devices," *IEEE Trans. Mob. Comput.*, vol. 19, no. 6, pp. 1387–1400, 2020.

[9] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *MOBICOM 2000, Proceedings of the sixth annual international conference on Mobile computing and networking, Boston, MA, USA, August 6-11, 2000*. ACM, 2000, pp. 255–265.

[10] E. Hernández-Orallo, M. D. S. Olmos, J. Cano, C. T. Calafate, and P. Manzoni, "Cocowa: A collaborative contact-based watchdog for detecting selfish nodes," *IEEE Trans. Mob. Comput.*, vol. 14, no. 6, pp. 1162–1175, 2015.

[11] J. A. F. F. Dias, J. J. P. C. Rodrigues, F. Xia, and C. X. Mavromoustakis, "A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks," *IEEE Trans. Ind. Electron.*, vol. 62, no. 12, pp. 7929–7937, 2015.

[12] B. Jedari, F. Xia, H. Chen, S. K. Das, A. Tolba, and Z. Al-Makhadmeh, "A social-based watchdog system to detect selfish nodes in opportunistic mobile networks," *Future Gener. Comput. Syst.*, vol. 92, pp. 777–788, 2019.

[13] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks," *IEEE Trans. Parallel Distributed Syst.*, vol. 25, no. 1, pp. 22–32, 2014.

[14] J. Cho and I. Chen, "PROVEST: provenance-based trust model for delay tolerant networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 15, no. 1, pp. 151–165, 2018.

[15] J. Choi, K. Shim, S. Lee, and K. Wu, "Handling selfishness in replica allocation over a mobile ad hoc network," *IEEE Trans. Mob. Comput.*, vol. 11, no. 2, pp. 278–291, 2012.

[16] Y. Li, G. Su, D. O. Wu, D. Jin, L. Su, and L. Zeng, "The impact of node selfishness on multicasting in delay tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 5, pp. 2224–2238, 2011.

[17] S. Basu, A. Biswas, S. Roy, and S. D. Bit, "Wise-prophet: A watchdog supervised prophet for reliable dissemination of post disaster situational information over smartphone based DTN," *J. Netw. Comput. Appl.*, vol. 109, pp. 11–23, 2018.

[18] B. Gao, T. Maekawa, D. Amagata, and T. Hara, "Environment-adaptive malicious node detection in manets with ensemble learning," in *38th IEEE International Conference on Distributed Computing Systems, ICDCS 2018, Vienna, Austria, July 2-6, 2018*. IEEE Computer Society, 2018, pp. 556–566.

[19] N. Nomikos, T. Charalambous, D. Vouyioukas, R. Wichman, and G. K. Karagiannidis, "Integrating broadcasting and NOMA in full-duplex buffer-aided opportunistic relay networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9157–9162, 2020.

[20] A. Chhabra, V. Vashishth, and D. K. Sharma, "SEIR: A stackelberg game based approach for energy-aware and incentivized routing in selfish opportunistic networks," in *51st Annual Conference on Information Sciences and Systems, CISS 2017, Baltimore, MD, USA, March 22-24, 2017*. IEEE, 2017, pp. 1–6.

[21] K. Chen, H. Shen, and L. Yan, "Multicent: A multifunctional incentive scheme adaptive to diverse performance objectives for DTN routing," *IEEE Trans. Parallel Distributed Syst.*, vol. 26, no. 6, pp. 1643–1653, 2015.

[22] Y. Mao and P. Zhu, "A game theoretical model for energy-aware DTN routing in manets with nodes' selfishness," *Mob. Networks Appl.*, vol. 20, no. 5, pp. 593–603, 2015.

[23] G. Costantino, R. R. Maiti, F. Martinelli, and P. Santi, "Losero: A locality sensitive routing protocol in opportunistic networks with contact profiles," *IEEE Trans. Mob. Comput.*, vol. 19, no. 10, pp. 2392–2408, 2020.

[24] K. Sakai, M. Sun, W. Ku, J. Wu, and F. S. Alanazi, "An analysis of onion-based anonymous routing for delay tolerant networks," in *36th IEEE International Conference on Distributed Computing Systems, ICDCS 2016, Nara, Japan, June 27-30, 2016*. IEEE Computer Society, 2016, pp. 609–618.

[25] N. Magaia, C. Borrego, P. R. Pereira, and M. Correia, "eprivo: An enhanced privacy-preserving opportunistic routing protocol for vehicular delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11 154–11 168, 2018.

[26] H. Zheng and J. Wu, "Up-and-down routing through nested core-periphery hierarchy in mobile opportunistic social networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4300–4314, 2017.

[27] E. Rosas, F. Garay, and N. Hidalgo, "Context-aware self-adaptive routing for delay tolerant network in disaster scenarios," *Ad Hoc Networks*, vol. 102, p. 102095, 2020.

[28] H. Z. S. T. C. C. H. Zhou, J. Wu and J. Chen, "Incentive-driven and freshness-aware content dissemination in selfish opportunistic mobile networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 9, pp. 2493–2505, 2015.

[29] M. C. I. R. Chen, F. Bao and J. H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, 2014.

[30] Z. W. H. Chen, W. Lou and Q. Wang, "A secure credit-based incentive mechanism for message forwarding in noncooperative dtns," *IEEE Transactions on Vehicular Technology*, 2016.

[31] T. N. D. Pham and C. K. Yeo, "Detecting colluding blackhole and greyhole attacks in delay tolerant networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 5, pp. 1116–1129, 2016.

[32] S. Saha, S. Nandi, R. Verma, S. Sengupta, K. Singh, V. Sinha, and S. K. Das, "Design of efficient lightweight strategies to combat dos attack in delay tolerant network routing," *Wireless Networks*, 2018.

[33] S. Trifunovic and A. Hossmann-Picu, "Stalk and lie: The cost of sybil attacks in opportunistic networks," *Computer Communications*, vol. 73, no. JAN.1, pp. 66–79, 2016.

[34] L. Yao, Y. Man, Z. Huang, J. Deng, and X. Wang, "Secure routing based on social similarity in opportunistic networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 594–605, 2016.

[35] I. R. Chen, F. Bao, and J. Guo, "Trust-based service management for social internet of things systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 6, pp. 684–696, 2016.

[36] Y. Wu, S. Deng, and H. Huang, "Control of message transmission in delay/disruption tolerant network," *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 1, pp. 132–143, 2018.

[37] ——, "Control of message transmission in delay/disruption tolerant network," *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 1, pp. 132–143, 2018.

[38] X. Zhang, G. Neglia, J. F. Kurose, and D. F. Towsley, "Performance modeling of epidemic routing," *Comput. Networks*, vol. 51, no. 10, pp. 2867–2891, 2007.